JC17 Rec'd PCT/PTO 28 JUN 2001

FORM PTO-1390 (Modified)
(REV 11-2000)

U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

# TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER
**T2146-907343**

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR
09/869435

| INTERNATIONAL APPLICATION NO. | INTERNATIONAL FILING DATE | PRIORITY DATE CLAIMED |
|---|---|---|
| **PCT/FR00/02978** | **October 26, 2000** | **October 28, 1999** |

TITLE OF INVENTION
**Method for Protecting an Electronic System with Modular Exponentiation-Based Cryptography Against Attacks by Physical Analysis**

APPLICANT(S) FOR DO/EO/US
**Louis GOUBIN**

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include itens (5), (6), (9) and (24) indicated below.
4. ☒ The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. ☒ A copy of the International Application as filed (35 U.S.C. 371 (c) (2))
   a. ☐ is attached hereto (required only if not communicated by the International Bureau).
   b. ☒ has been communicated by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☒ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
   a. ☐ is attached hereto.
   b. ☒ has been previously submitted under 35 U.S.C. 154(d)(4).
7. ☐ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371 (c)(3))
   a. ☐ are attached hereto (required only if not communicated by the International Bureau).
   b. ☐ have been communicated by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☐ have not been made and will not be made.
8. ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371 (c)(4)).
10. ☐ An English language translation of the annexes of the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371 (c)(5)).
11. ☐ A copy of the International Preliminary Examination Report (PCT/IPEA/409).
12. ☒ A copy of the International Search Report (PCT/ISA/210).

**Items 13 to 20 below concern document(s) or information included:**

13. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
14. ☒ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
15. ☒ A **FIRST** preliminary amendment.
16. ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
17. ☐ A substitute specification.
18. ☒ A change of power of attorney and/or address letter.
19. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.
20. ☐ A second copy of the published international application under 35 U.S.C. 154(d)(4).
21. ☐ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
22. ☐ Certificate of Mailing by Express Mail
23. ☐ Other items or information:

    **Verification of Translator**
    **Formal Drawings (1)**
    **Proposed Drawing Corrections, with 1 red-lined formal drawing**
    **PCT forms: Demande, PCT/IB/301, 308; PCT/RO/101**

JC03 Rec'd PCT/PTC 28 JUN 2001

| U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR | INTERNATIONAL APPLICATION NO. | ATTORNEY'S DOCKET NUMBER |
|---|---|---|
| 09/869435 | PCT/FR00/02978 | T2146-907343 |

24. The following fees are submitted:.

**BASIC NATIONAL FEE ( 37 CFR 1.492 (a) (1) - (5)) :**

| | | CALCULATIONS | PTO USE ONLY |
|---|---|---|---|
| ☐ Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO ............ | $1000.00 | | |
| ☒ International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO ........ | $860.00 | | |
| ☐ International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO ............ | $710.00 | | |
| ☐ International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4) ............ | $690.00 | | |
| ☐ International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4) .......... | $100.00 | | |
| **ENTER APPROPRIATE BASIC FEE AMOUNT =** | | $860.00 | |
| Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (e)). | | $0.00 | |

| CLAIMS | NUMBER FILED | NUMBER EXTRA | RATE | | |
|---|---|---|---|---|---|
| Total claims | 11 - 20 = | 0 | x $18.00 | $0.00 | |
| Independent claims | 3 - 3 = | 0 | x $80.00 | $0.00 | |
| Multiple Dependent Claims **(check if applicable).** | | | ☐ | $0.00 | |
| **TOTAL OF ABOVE CALCULATIONS =** | | | | $860.00 | |
| ☐ Applicant claims small entity status. (See 37 CFR 1.27). The fees indicated above are reduced by 1/2. | | | | $0.00 | |
| **SUBTOTAL =** | | | | $860.00 | |
| Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (f)). + | | | | $0.00 | |
| **TOTAL NATIONAL FEE =** | | | | $860.00 | |
| Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31) **(check if applicable).** | | | ☒ | $40.00 | |
| **TOTAL FEES ENCLOSED =** | | | | $900.00 | |
| | | | | **Amount to be: refunded** | $ |
| | | | | **charged** | $ |

a. ☒ A check in the amount of $900.00 to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. ________ in the amount of ________ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 50-1165 A duplicate copy of this sheet is enclosed.

d. ☐ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. **Credit card information should not be included on this form.** Provide credit card information and authorization on PTO-2038.

**NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.**

SEND ALL CORRESPONDENCE TO:

**Edward J. Kondracki**
**MILES & STOCKBRIDGE P.C.**
**Suite 500 - 1751 Pinnacle Drive**
**McLean, VA 22102-3833**

Edward J. Kondracki
SIGNATURE

**Edward J. Kondracki**
NAME

**20,604**
REGISTRATION NUMBER

**June 28, 2001**
DATE

09/869435
JC03 Rec'd PCT/PTO 28 JUN 2001

T2146-907343-US 3857/BC(PCT)

**IN THE UNITED STATES DESIGNATED/ELECTED OFFICE (D.O./E.O./US)**

Applicant: Louis GOUBIN

International Application No.: PCT/FR00/02978

International Filing Date: 26 October 2000

U.S. Serial No.: To be Assigned

U.S. Filing Date: June 28, 2001

For: **SECURITY METHOD FOR A CRYPTOGRAPHIC ELECTRONIC ASSEMBLY BASED ON MODULAR EXPONENTIATION AGAINST ANALYTICAL ATTACKS**

McLean, Virginia

**PRELIMINARY AMENDMENT**

Honorable Commissioner of Patents
and Trademarks
Washington, D.C. 20231

Sir:

Please amend the subject application, filed concurrently herewith, as indicated below:

**IN THE TITLE:**

Please cancel the title in its entirety and substitute the following new title:

**-- METHOD FOR PROTECTING AN ELECTRONIC SYSTEM WITH MODULAR EXPONENTIATION-BASED CRYPTOGRAPHY AGAINST ATTACKS BY PHYSICAL ANALYSIS--**

**IN THE SPECIFICATION:**

After the title and before the first paragraph on page 1 at line 5, insert the following heading at the left-hand margin:

--<u>FIELD OF THE INVENTION</u>--;

Page 1, at line 13, insert the following heading at the left-hand margin:

--<u>BACKGROUND OF THE INVENTION</u>--;

Page 7, at line 13, insert the following heading and sentence:

--<u>BRIEF DESCRIPTION OF THE DRAWING</u>

Fig. 1 is a representation of a smart card.—

Page 7, delete the two paragraphs beginning at line 15 and ending at line 33 in their entirety and insert the following new paragraphs. (Paragraphs showing the changes using underlining and bracketing are included as an attachment at the end of this Preliminary Amendment).

--The invention can be implemented in any electronic system performing a cryptographic calculation involving a modular exponentiation, including a smart card 8 as shown in Fig. 1. The chip includes information processing means 9, connected on one end to a nonvolatile memory 10 and a volatile working memory RAM 11, and connected on another end to means 12 for cooperating with an information processing device. The nonvolatile memory 10 can comprise a non-modifiable ROM part and a modifiable part constituted by an EPROM, an EEPROM or a RAM of the "flash" type, or FRAM, (the latter being a ferromagnetic RAM)), i.e., having the characteristics of an EEPROM but with access times identical to those of a standard RAM.

For the chip, it is possible to use, in particular, a self-programmable microprocessor with a nonvolatile memory, as described in U.S. patent No. 4,382,279 assigned to the assignee of the present invention. In a variant, the microprocessor of the chip is replaced, or at least supplemented, by logical circuits installed in a semiconductor chip. In essence, such circuits are capable of performing calculations, including authentication and signature calculations, as a result of hard-wired, rather than microprogrammed, electronics. In particular, they can be of the ASIC ("Application Specific Integrated Circuit") type. Advantageously, the chip is designed in monolithic form.--

Page 8, after line 22, insert the following new paragraph:

--While this invention has been described in conjunction with specific embodiments thereof, it is evident that many alternatives, modifications and variations will be apparent to those skilled in the art. Accordingly, the preferred embodiments of the invention as set forth herein, are intended to be illustrative, not limiting. Various changes may be made without departing from the true spirit and full scope of the invention as set forth herein and defined in the claims.—

**<u>IN THE CLAIMS</u>:**

Please amend claims 1 – 7, and add new claims 8-11. The claims that follow are a complete set of "clean" claims. The original claims 1-7 marked up to show the changes with underlining and bracketing are included as an attachment to this Preliminary Amendment:

1. (Amended) A method for protecting an electronic system implementing a cryptographic process involving calculation of a modular exponentiation of a quantity (*x*), said modular exponentiation using a secret exponent (*d*), comprising breaking down said secret exponent (*d*) into a plurality of *k* unpredictable values ($d_1$, $d_2$, ..., $d_k$), the sum of which is equal to said secret exponent.

2. (Amended) A method according to claim 1, characterized in that said unpredictable values ($d_1$, $d_2$, ..., $d_k$), are obtained by:

a) deriving *(k-1)* values by means of a random generator; and

b) taking the difference between the secret exponent and the *(k-1)* values to derive a final value.

3. (Amended) A method according to claim 1, wherein calculation of the modular exponentiation is performed by:

a) raising the quantity (*x*) by an exponent comprising said value to obtain a set of results for each of said *k* values and

b) calculating a product of the results obtained in step a).

4. (Amended) A method according to claim 1, wherein at least one of said *(k-1)* values is obtained by means of a random generator and has a length

at least equal to 64 bits.

5. (Amended) Utilizing the method according to claim 1 in a smart card comprising information processing means.

6. (Amended) Utilizing the method according to claim 1 for protecting a cryptographic calculation process using the RSA algorithm.

7. (Amended) Utilizing the method according to claim 1 for protecting a cryptographic calculation process using the Rabin algorithm.

Please add the following new claims:

--8. (New claim) A method for protecting an electronic system implementing a cryptographic process involving calculation of a modular exponentiation of a quantity ($x$), said modular exponentiation using a secret exponent ($d$), comprising breaking down said secret exponent ($d$) into a plurality of $k$ unpredictable values ($d_1$, $d_2$, ..., $d_k$), the sum of which is equal to said secret exponent; obtaining said unpredictable values ($d_1$, $d_2$, ..., $d_k$) by deriving $(k-1)$ values by means of a random generator; by raising the quantity ($x$) by an exponent comprising a final value and obtaining a set of results for each of said k values and calculating a product of the set of results and taking the difference between the secret exponent and the $(k-1)$ values to derive the final value.

9. (New Claim) A method according to claim 8, wherein at least one of said $(k-1)$ values is obtained by means of a random generator and has a length at least equal to 64 bits.

10. (New Claim) A smart card adapted to protect an electronic system comprising means for implementing a cryptographic process involving calculation of a modular exponentiation of a quantity ($x$), said modular exponentiation using a secret exponent ($d$), comprising breaking down said secret exponent ($d$) into a plurality of $k$ unpredictable values ($d_1$, $d_2$, ..., $d_k$), the sum of which is equal to said secret exponent, means for obtaining said unpredictable values ($d_1$, $d_2$, ..., $d_k$) by a random generator for deriving $(k-1)$ values and means for taking the

difference between the secret exponent and the *(k-1)* values to derive a final value.

11. (New Claim) A smart card according to claim 10, wherein calculation of the modular exponentiation is performed by:

a) raising the quantity ($x$) by an exponent comprising said value to obtain a set of results for each of said $k$ values and

b) calculating a product of the results obtained.--

**IN THE ABSTRACT:**

Please delete the Abstract at page 11 in its entirety and substitute the following new Abstract.

## --ABSTRACT

The invention concerns a method for protecting an electronic system implementing a cryptographic calculation process involving a modular exponentiation of a quantity ($x$), said modular exponentiation using a secret exponent ($d$), characterized in that said secret exponent is broken down into a plurality of $k$ unpredictable values ($d_1$, $d_2$, ..., $d_k$), the sum of which is equal to said secret exponent.--

## REMARKS

This Preliminary Amendment is filed to insert headings to conform the application to U.S. practice and to correct informalities in the specification, claims and abstract resulting from a literal translation of the French text.

Early action on the merits is earnestly solicited.

Respectfully submitted,

MILES & STOCKBRIDGE P.C.

Date: June 28, 2001

By: ______________________
Edward J. Kondracki
Registration No. 20,604

1751 Pinnacle Drive – Suite 500
McLean, VA 22102-3833
Tel.: 703/903-9000
Fax: 703/610-8686

**The following are the two paragraphs on page 7 beginning at line 15 and ending at line 33 showing the changes made using underlining and bracketing:**

The invention can be implemented in any electronic system performing a cryptographic calculation involving a modular exponentiation, including a smart card 8 as [in the sole figure] shown in Fig. 1. The chip includes information processing means 9, connected on one end to a nonvolatile memory 10 and a volatile working memory RAM 11, and connected on another end to means 12 for cooperating with an information processing device. The nonvolatile memory 10 can comprise a non-modifiable ROM part and a modifiable part constituted by an EPROM, an EEPROM or a RAM of the "flash" type, or FRAM, (the latter being a ferromagnetic RAM)), i.e., having the characteristics of an EEPROM but with access times identical to those of a standard RAM.

For the chip, it is possible to use, in particular, a self-programmable microprocessor with a nonvolatile memory, as described in U.S. patent No. 4,382,279 [in the name of the Applicant] assigned to the assignee of the present invention. In a variant, the microprocessor of the chip is replaced, or at least supplemented, by logical circuits installed in a semiconductor chip. In essence, such circuits are capable of performing calculations, including authentication and signature calculations, as a result of hard-wired, rather than microprogrammed, electronics. In particular, they can be of the ASIC ("Application Specific Integrated Circuit") type. Advantageously, the chip is designed in monolithic form.

**The following are the amended claims marked up to show the changes with underlining and bracketing:**

1. (Amended) [Method] A method for protecting an electronic system implementing a cryptographic [calculation] process involving calculation of a modular exponentiation of a quantity (*x*), said modular exponentiation using a secret exponent (*d*), [characterized in that] comprising breaking down said secret exponent [is broken down] (*d*) [in to] into a plurality of *k* unpredictable values ($d_1$, $d_2$, …, $d_k$), the sum of which is equal to said secret exponent.

2. (Amended) [Method] A method according to claim 1, characterized in that said unpredictable values ($d_1$, $d_2$, …, $d_k$), are obtained [in the following way] by:

a) deriving *(k-1)* values [are obtained] by means of a random generator; and

b) taking [the final value is obtained from] the difference between the secret exponent and the *(k-1)* values to derive a final value.

3. (Amended) [Method] A method according to claim 1, [characterized in that the] wherein calculation of the modular exponentiation is performed [in the following way] by:

a) [for each of said *k* values,] raising the quantity (*x*) [is raised] by an exponent comprising said value [in order] to obtain [a result,] a set of results [thus being obtained] for each of said *k* values; and

b) calculating a product of the results obtained in step a) [is calculated].

4. (Amended) [Method] A method according to claim 1, [characterized in that] wherein at least one of said *(k-1)* values is obtained by means of a random generator and has a length [greater than or] at least equal to 64 bits.

5. (Amended) [Utilization of] Utilizing the method according to claim 1 in a smart card comprising information processing means.

6. (Amended) [Utilization of] Utilizing the method according to claim 1 [to protect] for protecting a cryptographic calculation process using the RSA algorithm.

7. (Amended) [Utilization of] Utilizing the method according to claim 1 [to protect] for protecting a cryptographic calculation process using the Rabin algorithm.

# SECURITY METHOD FOR A CRYPTOGRAPHIC ELECTRONIC ASSEMBLY BASED ON MODULAR EXPONENTIATION AGAINST ANALYTICAL ATTACKS

The present invention relates to a method for protecting an electronic system implementing an algorithm involving a modular exponentiation, in which the exponent is secret. More precisely, the purpose of the method is to create a version of such an algorithm that is not vulnerable to a certain type of physical attack - called *Differential Power Analysis* or *High-Order Differential Power Analysis*, (abbreviated DPA or HO-DPA) – which tries to obtain information on the secret key from a study of the electric power consumption of the electronic system during the execution of the calculation.

The cryptographic algorithms considered herein use a secret key to calculate a piece of output information based on a piece of input information; this can involve an encryption, decryption, signature, signature verification, authentication, non-repudiation or key-exchange operation. They are constructed in such a way that a hacker, knowing the inputs and the outputs, cannot in practice deduce any information on the secret key itself.

We are therefore interested in a class larger than that traditionally designated by the expression *secret key algorithms* or *symmetrical algorithms*. In particular, everything described in the present patent application also applies to so-called *public key* or *asymmetrical algorithms*, which actually include two keys: one public, the other private and not divulged, the latter being the one targeted by the attacks described below.

Attacks of the Power Analysis type, developed by Paul Kocher and *Cryptographic Research* (see the document *Introduction to Differential Power Analysis and Related Attacks* by Paul Kocher, Joshua Jaffe, and Benjamin Jun, Cryptography Research, 870 Market St., Suite 1008, San Francisco, CA 94102; HTML edition of the document available at the URL address: http://www.cryptography.com/dpa/technical/index.html) start with the observation that in reality the hacker can acquire information other than simply the input and output data during the execution of the calculation, such as for example the power

consumption of the microcontroller or the electromagnetic radiation emitted by the circuit.

Differential power analysis is an attack that makes it possible to obtain information on the secret key contained in the electronic system, by performing a statistical analysis of the power consumption records, performed on a large number of calculations with this same key.

This attack does not require any knowledge of the individual power consumption of each instruction, or on the temporal position of each of these instructions. It applies in the same way assuming that the hacker knows some of the outputs of the algorithm and the corresponding consumption curves. It is based solely on the fundamental hypothesis according to which:

*<u>Fundamental hypothesis</u>: There is an intermediate variable appearing during the calculation of the algorithm, such that the knowledge of a few key bits, in practice less than 32 bits, makes it possible to decide whether or not two inputs, respectively two outputs, give the same value for this variable.*

The so-called high-order power analysis attacks are a generalization of the DPA attack described above. They can use several different sources of information: in addition to the consumption, they can use measurements of electromagnetic radiation, temperature, etc., performing statistical operations that are more sophisticated than the simple notion of an average, and intermediate variables that are less elementary than a simple bit or a simple byte. Nevertheless, they are based on exactly the same fundamental hypothesis as DPA.

The object of the method that is the subject of the present invention is to eliminate the risk of DPA or HO-DPA attacks on electronic systems with secret or private key cryptography involving modular exponentiation in which the exponent is secret.

Another object of the present invention is consequently to modify the cryptographic calculation process implemented by protected electronic cryptographic systems, in such a way that the aforementioned fundamental hypothesis is not longer verified, i.e. that there is no intermediate variable that depends on the consumption of a sub-system easily accessible by the secret or private key, attacks of the DPA or HO-DPA thus being rendered ineffective.

## First example: the RSA algorithm

RSA is the most famous of the asymmetrical cryptographic algorithms. It was developed by Rivest, Shamir and Adleman in 1978. For a more detailed description of this algorithm, it may be useful to refer to the following document:

- R.L. Rivest, A. Shamir, L.M. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM, 21, No. 2, 1978, pp. 120-126,

or to the following documents:

- ISO/IEC 9594-8/ITU-T X.509, *Information Technology – Open systems Interconnection – The Directory: Authentication Framework;*
- ANSI X9.31.1, *American National Standard, Public-Key Cryptography Using Reversible Algorithms for the Financial Services Industry*, 1993;
- PKCS #1, *RSA Encryption Standard*, version 2, 1998, available at the following address: ftp://ftp.rsa.com/pub/pkcs/doc/pkcs-1v2.doc.

The RSA algorithm uses a whole number $n$ that is the product of two large prime numbers $p$ and $q$, and a whole number $e$, prime with $ppcm(p-1, q-1)$, and such that $e \bullet \pm 1$ mod $ppcmp-1, q-1)$. The whole numbers $n$ and $e$ constitute the public key. The public key calculation uses the function $g$ of $\mathbf{Z}/nz$ in $\mathbf{Z}/n\mathbf{Z}$ defined by $g(x)=x^e$ mod $n$. The secret key calculation uses the function $g^{-1}(y)=y^d$ mod $n$, where $d$ is the secret exponent (also called the secret or private key) defined by $ed \bullet 1$ mod $ppcm(p-1, q-1)$.

Attacks of the DPA or HO-DPA type can pose a threat to the standard implementations of the RSA algorithm. In essence, the latter very often use the so called *square and multiply* principle to perform the calculation of $x^d \bmod n$.

This principle consists of writing the breakdown

$d = b_{m-1} \cdot 2^{m-1} + b_{m-2} \cdot 2^{m-2} + \ldots + b_1 \cdot 2^1 + b_0 \cdot 2^0$

of the secret exponent $d$ in base 2, the performing the calculation in the following way:

1. $z \bullet 1$;

for $i$ running from $m-1$ to $0$ perform:

2. $z \bullet z^2$ mod $n$;

3. if $b_i = 1$ then $z \bullet z \times x$ mod $n$.

In this calculation, it is clear that among the successive values assumed by the variable $z$, the prime numbers depend on only a few bits of the secret key $d$. The fundamental hypothesis that makes the DPA attack possible is therefore fulfilled. It is thus possible to guess, for example, the 10 high-order bits of $d$ by concentrating on the consumption measurements in the part of the algorithm that corresponds to $i$ running from $m-1$ to $m-10$, which makes it possible to find the next ten bits of $d$, and so on. Eventually, all the bits of the secret exponent $d$ are found.

## A first protection method, and its disadvantages

A conventional method (proposed by Ronald Rivest in 1995) for protecting the RSA algorithm against DPA type attacks consists of using a "blinding" principle. This uses the fact that:

$x^d \bmod n = (x \times r^e)^d \times r^{-1} \bmod n$

Thus, the calculation of $y = x^d \bmod n$ is broken down into four steps:

- A random generator is used to obtain a value $r$ ;
- We calculate : $u = x \times r^e \bmod n$ ;
- We calculate : $v = u^d \bmod n$ ;
- We calculate : $y = v \times r^{-1} \bmod n$.

The disadvantage of this method is that it makes it necessary, for each calculation, to calculate the modular inverse $r^{-1}$ of the random value $r$, this operation generally being time-consuming (the duration of such a calculation is on the same order as that of a modular exponentiation such as $u^d \bmod n$). Consequently, this new implementation (protected against DPA attacks) of the calculation of $x^d \bmod n$ takes about twice as long as the initial implementation (not protected against DPA attacks). In other words, this protection of RSA against DPA attacks increases the calculation time by approximately **100%** (assuming that the public exponent $e$ is very small, for example $e=3$; if the exponent $e$ is larger, this calculation time is even longer).

## A second method: the method of the present invention

According to the invention, a method for protecting an electronic system implementing a cryptographic calculation process involving a modular exponentiation

of a quantity ($x$), said modular exponentiation using a secret exponent ($d$), is characterized in that said secret exponent is broken down into a plurality of $k$ unpredictable values ($d_1, d_2, \ldots, d_k$), the sum of which is equal to said secret exponent.

Advantageously, said values ($d_1, d_2, \ldots, d_k$), are obtained in the following way:

a) ($k$-$1$) values are obtained by means of a random generator;

b) the final value is obtained from the difference between the secret exponent and the ($k$-$1$) values.

Advantageously, the calculation of the modular exponentiation is performed in the following way:

a) for each of said $k$ values, the quantity ($x$) is raised by an exponent comprising said value in order to obtain a result, a set of results thus being obtained;

b) a product of the results obtained in step a) is calculated.

Advantageously, at least one of said ($k$-$1$) values obtained by means of a random generator has a length greater than or equal to 64 bits.

Some of the details and advantages of the present invention will emerge from the following description of some preferred but non-limiting embodiments, in reference to the sole attached figure, which represents a smart card.

According to the invention, we use the fact that:

if $d = d_1 + d_2$, then $x^d \; mod \; n = x^{d_1} \times x^{d_2} \; mod \; n$

Thus, the calculation of $y = x^d \; mod \; n$ is broken down into five steps:

- A random generator is used to obtain a value $d_1$ ;
- We calculate : $d_2 = d - d_1$ ;
- We calculate : $u = x^{d_1} \; mod \; n$ ;
- We calculate : $v = x^{d_2} \; mod \; n$ ;
- We calculate : $y = u \times v \; mod \; n$.

The advantage is that, this way, there is no modular inverse to calculate. In general, the calculation time of a modular exponentiation is proportional to the size of the exponent. Thus, if we let • be the ratio between the size of $d_1$ and the size of $d_2$, it is clear that the total calculation time in this new implementation (protected against DPA attacks) is about ($1$+• ) times the calculation time in the initial implementation (not protected against DPA attacks).

Note that, in order to obtain an unpredictable value $d_1$, it necessary for its size to be at least 64 bits.

The method thus described renders attacks of the DPA or HO-DPA type described above ineffective. In essence, in deciding whether or not two inputs (respectively two outputs) of the algorithm give the same value for an intermediate variable appearing during the calculation, it is no longer enough to know the key bits involved. It is also necessary to know the breakdown of the secret key $d$ into $k$ values $d_1, d_2, \ldots, d_k$ such that $d=d_1+d_2+ \ldots +d_k$. Assuming that this breakdown is secret, and that at least one of the $k$ values has a size of at least 64 bits, the hacker cannot predict the values of $d_1, \ldots, d_k$, and therefore the fundamental hypothesis that would make it possible to implement a DPA or HO-DPA type attack, is no longer verified.

Examples:

1. If $n$ has a length of 512 bits, by choosing to take a random value $d_1$ of 64 bits, we obtain • $=1/8$, which means that this protection of RSA against DPA attacks increases the calculation time by about **12.5%**.

2. If $n$ has a length of 1024 bits, by choosing to take a random value $d_1$ of 64 bits, we obtain • $=1/16$, which means that this protection of RSA against DPA attacks increases the calculation time by about **6.25%**.

## Second example: the Rabin algorithm

We will now consider the asymmetrical cryptographic algorithm developed by Rabin in 1979. For a more detailed description of this algorithm, it may be useful to refer to the following document:

- M. O. Rabin, *Digitized Signatures and Public-Key Functions as Intractable as Factorization*, Technical Report LCS/TR-212, M.I.T. Laboratory for Computer Science, 1979.

The Rabin algorithm uses a whole number $n$ that is the product of two large prime numbers $p$ and $q$, which also verify the following two conditions:

- $p$ is congruent with 3 modulo 8 ;
- $q$ is congruent with 7 modulo 8.

The public key calculation uses the function g of **Z**/n**Z** in **Z**/n**Z** defined by $g(x)=x^2 \bmod n$. The secret key calculation uses the function $g^{-1}(y)=y^d \bmod n$, where $d$

is the secret exponent (also called the secret or private key) defined by $d=((p-1)(q-1)/4+1)/2$.

The function implemented by the secret key calculation being exactly the same as that used by the RSA algorithm, the same DPA or HO-DPA attacks are applicable and can pose the same threats to the Rabin algorithm.

**<u>Protecting the algorithm</u>**

Since the function is exactly the same as the one in RSA, the protection method described in the RSA context is applied in the same way in the case of the Rabin algorithm. The increase in the calculation time caused by the application of this method is also the same as in the case of the RSA algorithm.

---

The invention can be implemented in any electronic system performing a cryptographic calculation involving a modular exponentiation, including a smart card 8 as in the sole figure. The chip includes information processing means 9, connected on one end to a nonvolatile memory 10 and a volatile working memory RAM 11, and connected on another end to means 12 for cooperating with an information processing device. The nonvolatile memory 10 can comprise a non-modifiable ROM part and a modifiable part constituted by an EPROM, an EEPROM or a RAM of the "flash" type, or FRAM, (the latter being a ferromagnetic RAM)), i.e., having the characteristics of an EEPROM but with access times identical to those of a standard RAM.

For the chip, it is possible to use, in particular, a self-programmable microprocessor with a nonvolatile memory, as described in U.S. patent No. 4,382,279 in the name of the Applicant. In a variant, the microprocessor of the chip is replaced, or at least supplemented, by logical circuits installed in a semiconductor chip. In essence, such circuits are capable of performing calculations, including authentication and signature calculations, as a result of hard-wired, rather than microprogrammed, electronics. In particular, they can be of the ASIC ("Application Specific Integrated Circuit") type. Advantageously, the chip is designed in monolithic form.

In the case of the utilization of such an electronic system, the invention consists in a method for protecting an electronic system comprising information processing means and information storage means, the method implementing a cryptographic calculation process involving a modular exponentiation of a quantity ($x$) stored in the information storage means, said modular exponentiation using a secret exponent ($d$) stored in the storage means, characterized in that, by means of said information processing means, said secret exponent read in said information storage means is broken down into a plurality of $k$ unpredictable values ($d_1$, $d_2$, ..., $d_k$), the sum of which is equal to said secret exponent, said $k$ unpredictable values being stored in the information storage means.

Advantageously, said values ($d_1$, $d_2$, ..., $d_k$) are obtained in the following way:

a) $(k-1)$ values are obtained by means of a random generator and stored in the information storage means;

b) the final value is obtained from the difference between the secret exponent and the $(k-1)$ values, calculated by means of said information processing means.

Advantageously, the calculation of the modular exponentiation is performed in the following way:

a) for each of said $k$ values, the quantity ($x$) is raised by an exponent comprising said value in order to obtain a result, a set of results thus being obtained;

b) a product of the results obtained in step a) is calculated.

Advantageously, at least one of said $(k-1)$ values obtained by means of a random generator has a length greater than or equal to 64 bits.

## CLAIMS

1. Method for protecting an electronic system implementing a cryptographic calculation process involving a modular exponentiation of a quantity ($x$), said modular exponentiation using a secret exponent ($d$), characterized in that said secret exponent is broken down in to a plurality of $k$ unpredictable values ($d_1, d_2, \ldots, d_k$), the sum of which is equal to said secret exponent.

2. Method according to claim 1, characterized in that said values ($d_1, d_2, \ldots, d_k$), are obtained in the following way:

a) $(k-1)$ values are obtained by means of a random generator;

b) the final value is obtained from the difference between the secret exponent and the $(k-1)$ values.

3. Method according to claim 1, characterized in that the calculation of the modular exponentiation is performed in the following way:

a) for each of said $k$ values, the quantity ($x$) is raised by an exponent comprising said value in order to obtain a result, a set of results thus being obtained;

b) a product of the results obtained in step a) is calculated.

4. Method according to claim 1, characterized in that at least one of said $(k-1)$ values obtained by means of a random generator has a length greater than or equal to 64 bits.

5. Utilization of the method according to claim 1 in a smart card comprising information processing means.

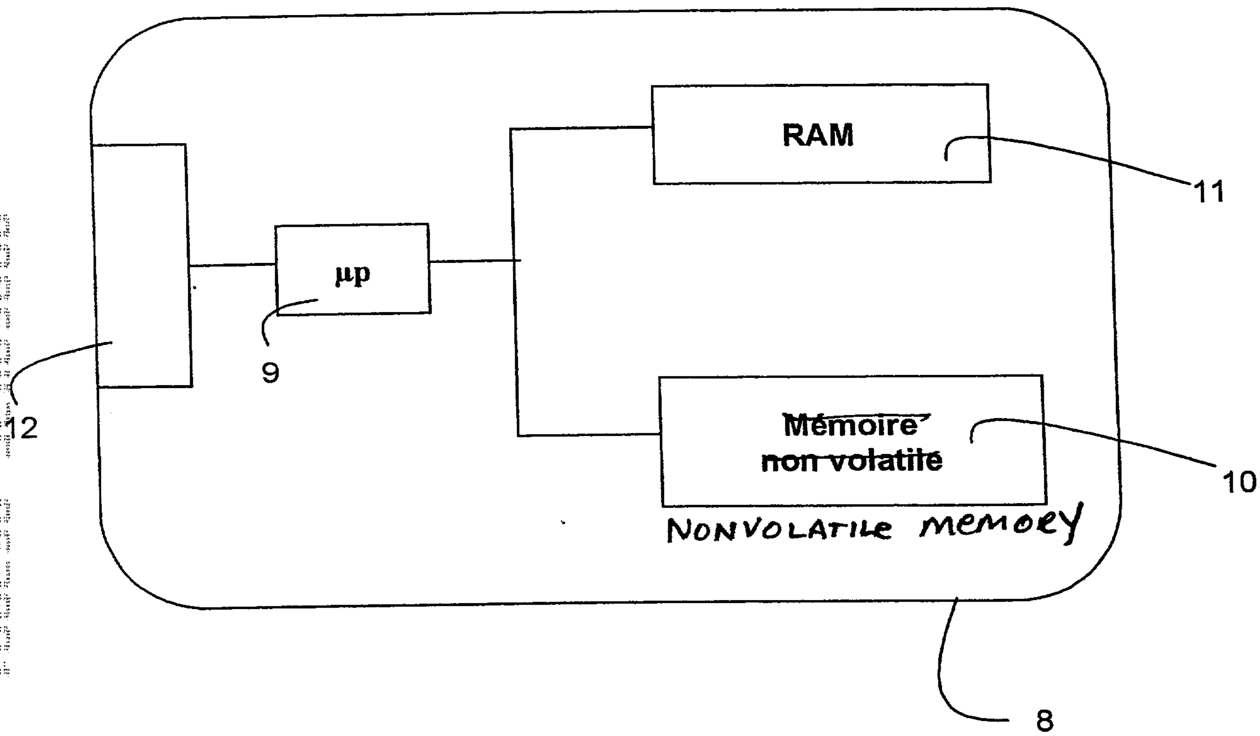
6. Utilization of the method according to claim 1 to protect a cryptographic calculation process using the RSA algorithm.

7. Utilization of the method according to claim 1 to protect a cryptographic calculation process using the Rabin algorithm.

## ABSTRACT

# SECURITY METHOD FOR A CRYPTOGRAPHIC ELECTRONIC ASSEMBLY BASED ON MODULAR EXPONENTIATION AGAINST ANALYTICAL ATTACKS

The invention concerns a method for protecting an electronic system implementing a cryptographic calculation process involving a modular exponentiation of a quantity ($x$), said modular exponentiation using a secret exponent ($d$), characterized in that said secret exponent is broken down into a plurality of $k$ unpredictable values ($d_1$, $d_2$, …, $d_k$), the sum of which is equal to said secret exponent.




~~FIGURE UNIQUE~~

SOLE FIGURE

US 03857/CORLU Bernard

# French Language Declaration

Je revendique par le présent acte le bénéfice de priorité étrangère selon Titre 35, du Code des Etats-Unis, §119 de toute demande de brevet ou d'attestation d'inventeur énumérée ci-après, et j'ai identifié également ci-après toute demande étrangère de brevet ou d'attestation d'inventeur ayant une date de dépôt antérieure à celle de la demande pour laquelle la priorité est revendiquée.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior foreign applications

Demande(s) de brevet antérieure(s) dans un autre pays:

Priority claimed / Droit de priorité revendiqué

| (Number) (Numéro) | (Country) (Pays) | (Day/Month/Year Filed) (Jour/Mois/Année de dépôt) | Yes Oui | No Non |
|---|---|---|---|---|
| FR 99 13507 | France | 28 10 1999 | ☒ | ☐ |
| | | | ☐ | ☐ |
| | | | ☐ | ☐ |

Je revendique par le présent acte, le bénéfice selon Titre 35 du Code des Etats-Unis, §120 de toute(s) demande(s) américaines énumérée(s) ci-après et, dans la mesure où le sujet de chacune des revendications de cette demande n'est pas divulgué dans la demande américaine antérieure, de la façon définie par le premier paragraphe de Titre 35 du Code des Etats-Unis, §112, je reconnais le devoir de divulguer l'information pertinente selon Titre 37 du Code des Réglements Fédéraux, §1.56(a), toute information qui se présente entre la date de dépôt de la demande antérieure et la date de dépôt de la demande, soit nationale, soit internationale PCT.

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

| (Application Serial No.) (No. de Demande) | (Filing Date) (Date de Dépôt) | (Etat) (breveté, pendante, abandonné) / (Status) (patented, pending, abandoned) |
|---|---|---|
| PCT/FR 00/02978 | 26/10/00 | PENDING |
| | | |

Je déclare par le présent acte que toutes mes déclarations, à ma connaissance, sont vraies et que toutes les déclarations faites à partir de renseignements ou de suppositions, sont tenues pour être vraies; de plus, toutes ces déclarations ont été faites en sachant que de fausses déclarations volontaires ou autres actes de même nature sont sanctionées par une amende ou un emprisonnement, ou les deux, selon la Section 1001, du Titre 18 de Code des Etats-Unis et que de telles déclarations délibérément fausses peuvent compromettre la validité de la demande ou du brevet délivré.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

US 03857/CORLU Bernard

# French Language Declaration

POUVOIR: En tant qu'inventeur, je désigne l'(les) avocat(s) et/ou l'(les) agent(s) suivant(s) pour poursuivre la procédure de cette demande et traiter toute affaire la concernant auprès du Bureau des Brevets et de Marques:

Harold L. Stowell, Reg. 17,233
Edward J. Kondracki, Reg. 20,604
Dennis P. Clarke, Reg. 22,549
William L. Feeney, Reg. 29,918
John C. Kerins, Reg. 32,421

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. (*list name and registration number*)

Harold L. Stowell, Reg. 17,233
Edward J. Kondracki, Reg. 20,604
Dennis P. Clarke, Reg. 22,549
William L. Feeney, Reg. 29,918
John C. Kerins, Reg. 32,421

10

Adresser toute correspondance à:

Edward J. Kondracki, Esq.
KERKAM, STOWELL, KONDRACKI
& CLARKE, P.C.
5203 Leesburg Pike, Suite 600
Falls Church, VA 22041

Send Correspondence to:

Edward J. Kondracki, Esq.
KERKAM, STOWELL, KONDRACKI
& CLARKE, P.C.
5203 Leesburg Pike, Suite 600
Falls Church, VA 22041

Adresser toute communication téléphonique à: (Nom) (Numéro de téléphone)

Edward J. Kondracki, Esq.
(703) 998-3302

Direct Telephone Calls to: (*name and telephone number*)

Edward J. Kondracki, Esq.
(703) 998-3302

| | |
|---|---|
| Nom complet du seul ou premier inventeur<br>-00 GOUBIN Louis | Full name of sole or first inventor |
| Signature de l'inventeur Date 21/06/01 | Inventor's signature Date |
| Domicile<br>3 rue Brown-Séquard 75015 PARIS FRANCE FRX | Residence |
| Nationalité<br>Française | Citizenship |
| Adresse Postale<br>3 rue Brown-Séquard 75015 PARIS FRANCE | Post Office Address |
| | |
| Nom complet du second co-inventeur, le cas échéant | Full name of second joint inventor, if any |
| Signature de l'inventeur Date | Second Inventor's signature Date |
| Domicile | Residence |
| Nationalité | Citizenship |
| Adresse Postale | Post Office Address |
| | |

(Fournir les mêmes renseignements et la signature de tout co-inventeur supplémentaire.)

(Supply similar information and signature for third and subsequent joint inventors.)

# Declaration and Power of Attorney For Patent Application
# Declaration Pour Demandes de Brevets Avec Pouvoirs

## French Language Declaration

En tant qu' inventeur nommé ci-après, Je déclare par le présent acte que:

As a below named inventor, I hereby declare that:

Mon nom, mon domicile, mon adresse postale, ma nationalité sont ceux qui figurent ci-après,

My residence, post office address and citizenship are as stated below next to my name,

Je déclare que je crois être l'inventeur original, premier et unique (si un seul nom figure sur le présent acte) ou un des co-inventeurs, originaux et premiers (si plusieurs noms figurent sur le present acte) du sujet revendiqué et pour liquel un brevet est demandé sur la base de l'invention intitulée·

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

**Procédé de sécurisation d'un ensemble électronique de cryptographie à base d'exponentiation modulaire contre les attaques par analyse physique.**

dont la description (cocher la case correspondante)

the specification of which (check one)

- [x] est annexée au présent acte.
- [ ] a été déposée ______________

Numéro de série de la demande ______________

et modifiée le ______________ (si approprié)

- [ ] is attached hereto.
- [ ] was filed on ______________ as

Application Serial No. ______________

and was amended on ______________ (if applicable)

Je déclare par le présent acte avoir examiné et compris le contenu de la description identifiée ci-dessus, revendications y compris, et le cas échéant telle que modifiée par l'amendment cité plus haut

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

Je reconnais le devoir de divulguer l'information qui est en rapport avec l'examen de cette demande selon Titre 37 du Code des Reglements Fédéraux §1.56(a).

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

T2146-907343-US 3857/BC(PCT)

**IN THE UNITED STATES DESIGNATED/ELECTED OFFICE (D.O./E.O./US)**

| | |
|---|---|
| Applicant: | Louis GOUBIN |
| International Application No.: | PCT/FR00/02978 |
| International Filing Date: | 26 October 2000 |
| U.S. Serial No.: | To be Assigned |
| U.S. Filing Date: | June 28, 2001 |
| For: | **METHOD FOR PROTECTING AN ELECTRONIC SYSTEM WITH MODULAR EXPONENTIATION-BASED CRYPTOGRAPHY AGAINST ATTACKS BY PHYSICAL ANALYSIS** |

McLean, Virginia

## CHANGE OF ADDRESS

Honorable Commissioner of Patents and Trademarks
Washington, D.C. 20231

Sir:

Effective immediately, please note our new correspondence address and telephone/fax numbers as follows:

Miles & Stockbridge P.C.
1751 Pinnacle Drive
Suite 500
McLean, VA 22102-3833
Telephone: 703-903-9000
Fax: 703-610-8686

Respectfully submitted,

MILES & STOCKBRIDGE P.C.

Date: June 28, 2001

By: Edward J. Kondracki

Edward J. Kondracki
Registration No. 20,604

1751 Pinnacle Drive – Suite 500
McLean, VA 22102-3833
Tel.: 703/903-9000
Fax: 703/610-8686

TYSO01.9149589v90l000001-#BRCH7l06\25\01